From: Moore, Desiree F.

Sent: Thursday, April 16, 2020 6:32 PM

To: DOJ: Attorney General

Subject: Notice of Security Incident

_____

To whom it may concern:

I write on behalf of my client, ExecuPharm Inc. (a US-based employee staffing company). On March 13, 2020, ExecuPharm experienced a data security incident that compromised select corporate and personnel information. Specifically, unknown individuals encrypted ExecuPharm servers and sought a ransom in exchange for decryption. As a result of this incident, nine (9) New Hampshire residents were potentially impacted. ExecuPharm has notified potentially impacted New Hampshire residents on an informal basis beginning on March 16, 2020 and thereafter (including by way of a dedicated internal micro-site with key information and developments), and will send formal notification letters pursuant to statute on April 17, 2020. A form of that notification letter is attached hereto.

Should you have any questions, please do not hesitate to contact me.

Best regards,

Desiree

Desiree Moore
Partner
K&L Gates LLP
desiree.moore@klgates.com

70 W. Madison St.
Suite 3100
Chicago, IL 60602
Phone: +1 312 781 6028
www.klgates.com

<<FirstName>> <<LastName>> <<Date>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Notice of Security Incident - Sample Letter to Data Subjects

Dear <<FirstName>> <<LastName>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On March 13, 2020, ExecuPharm experienced a data security incident that compromised select corporate and personnel information. Specifically, unknown individuals encrypted ExecuPharm servers and sought a ransom in exchange for decryption.

As part of this incident, ExecuPharm employees received phishing emails from the unknown individuals. Upon a thorough investigation, ExecuPharm determined that the individuals behind the encryption and the sending of these emails may have accessed and/or shared select personal information relating to ExecuPharm personnel, as well as personal information relating to select personnel of Parexel, whose information was stored on ExecuPharm's data network.

ExecuPharm has notified federal and local law enforcement authorities in the United States and retained leading third party cybersecurity firms to investigate the nature and scope of the incident. ExecuPharm is also in the process of notifying the relevant authorities as required.

What information was involved?

We believe the individuals behind this data security incident may have accessed employee files. As a result, the information that may have been involved includes: social security numbers, taxpayer ID/EIN, driver's license numbers, passport numbers, bank account numbers, credit card numbers, national insurance numbers, national ID numbers, IBAN/SWIFT numbers, and beneficiary information (including social security numbers).

For information about what was contained in your employee file, please contact: employeeinquiries@execupharm.com. Unauthorized access to such information may potentially lead to the misuse of your personal data to impersonate you and/or to commit, or allow third parties to commit, fraudulent acts such as securing credit in your name.

What we are doing.

ExecuPharm internal teams worked diligently with forensic consultants to rebuild the impacted servers from back up servers and have now fully restored and secured the ExecuPharm systems. This included the installation of forensic tools on all systems and the isolation of impacted systems until ExecuPharm could confirm that they were secure. ExecuPharm also implemented additional countermeasures to block further ransomware emails from entering the ExecuPharm environment. ExecuPharm also upgraded its security measures to prevent future attacks, including forced password resets, multi-factor authentication for remote access, and endpoint protection, detection, and response tools.

Additionally, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have potentially sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report,

Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https:// enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 31, 2020** to activate your identity monitoring services. If you have already activated these services, no further action on identity monitoring services is required, though we encourage you to review the "Additional Resources" section below for further steps you can take to help protect yourself.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-800-819-0974, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your Membership Number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Stowe Milhous
Vice President, FSP
ExecuPharm

Marty Mahoney
Senior Vice President, Associate General Counsel and Chief Compliance Officer
Parexel

Brian Thornton
Senior Vice President, FSP
Parexel

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.